AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1-9. (canceled)

10. (currently amended) A network attack detection system, ~~characterized in that~~ comprising the steps of:

examining a header of a packet in transmission; ~~is examined and~~

observing ~~the~~ values of one or more pre-specified fields in the packet header; ~~are observed,~~ and

in a case where ~~the~~ a number of distinct values observed in the pre-specified fields reaches a pre-specified threshold within a pre-specified time interval, ~~it is judged~~ judging that an unauthorized attack is in progress,

wherein ~~and this judgment~~ the judging is carried out based on ~~either~~ one of the following conditions:

(a) N(t) is the number of distinct values of the field observed within a pre-specified time interval from time t, $N(t_1)$ is the number of distinct values of the field observed within the pre-specified time interval from some time t_1 and if the ratio of N(t) to $N(t_1)$ is greater than[[,]] or equal to[[,]] ~~some~~ a first pre-specified threshold k_1, that is, if $N(t)/ N(t_1) \geq k_1$, the system will judge that an attack is in progress;

(b) P(t) is the number of packets in transmission within the pre-specified time interval from ~~some~~ time t, and if the ratio of the number of N(t) to P(t) is greater than[[,]] or equal to[[,]] ~~some~~ a second pre-specified threshold k_2, that is, $N(t)/P(t) \geq k_2$, the system will judge that an attack is in progress;

(c) $P(t_1)$ is the number of packets in transmission within the pre-specified time interval from some time t_1, and if the ratio of the coefficient computed in (b) above for the time t to that computed for the time t1, $\{N(t)/P(t)\} / \{N(t_1)/P(t_1)\}$, is greater than[[,]] or equal to[[,]] ~~some~~ a third pre-specified threshold k_3, that is, $\{N(t)/P(t)\} / \{N(t_1)/P(t_1)\} \geq k_3$, the system will judge that an attack is under progress;

(d) T(t) is the number of octets or bits in the packets in transmission within the pre-specified time interval from some time t, and if the ratio N(t) to T(t) is greater than[[,]] or equal to[[,]]~~some~~ a fourth pre-specified threshold k_4, that is, $N(t)/T(t) \geq k_4$, the system will judge that an attack is in progress.

11. (currently amended) The network attack detection system according to claim 10, ~~characterized in that~~ wherein arbitrary combinations of two or more header fields are allowed, and the number of distinct values observed for the resultant

composite field is used to compute the coefficient which is compared against the threshold.

12. (currently amended) The network attach detection system according to claim 10, ~~characterized in that~~ wherein ~~it is inferred that~~ an illegal attack is inferred to be underway when the Time To Live (TTL) value in the header field of a packet does not lie in the range of the values seen beforehand for the source address in the header of packets.

13. (currently amended) A network attack detection system, ~~characterized in that~~ wherein it is judged that an illegal attack has taken place by observing the values of the packet header fields, and when the number of distinct values seen in a combination of two or more header fields exceeds a pre-specified threshold value within a pre-specified time, it is judged that an attack is in progress.

14. (currently amended) The network attack detection system according to claim 13, ~~characterized in that~~ wherein the judgment is made that an attack is in progress, if the Time to Live (TTL) value in the header of the packet does not lie in the range of the values seen beforehand for the source address in the header of the packet.

15. (currently amended) The network attack tracking system according to claim 10, ~~characterized in that~~ wherein a source of the unauthorized attack is searched by ~~setting~~ deploying these systems at various places on the Internet.

16. (currently amended) The network attack tracking system according to claim 11, ~~characterized in that~~ wherein a source of the unauthorized attack is searched by ~~setting~~ deploying these systems at various places on the Internet.

17. (currently amended) The network attack tracking system according to claim 12, ~~characterized in that~~ wherein a source of the unauthorized attack is searched by ~~setting~~ deploying these systems at various places on the Internet.

18. (currently amended) The network attack tracking system according to claim 13, ~~characterized in that~~ wherein a source of the unauthorized attack is searched by ~~setting~~ deploying these systems at various places on the Internet.

19. (currently amended) The network attack tracking system according to claim 14, ~~characterized in that~~ wherein the source of the unauthorized attack is searched by ~~setting~~ deploying these systems at various places on the Internet.

20. (currently amended) A method ~~of~~ for detecting a network attack, comprising the steps of:

examining a pre-specified field in a header of a packet in transmission for distinct values; and

determining that an unauthorized attack is in progress based on an observed number of distinct values in the examined pre-specified header field reaching a pre-specified threshold within a pre-specified time interval, wherein,

the determination includes that at least one of the following conditions is satisfied

(a) N(t) is the number of the distinct values of the field observed within the pre-specified time interval from some time t, $N(t_1)$ is the number of distinct values of the field observed within the pre-specified time interval from some time t_1 and if the ratio of N(t) to $N(t_1)$ is greater than[[,]] or equal to[[,]] a first pre-specified threshold k_1, that is $N(t)/N(t_1) \geq k_1$, it will be judged that an attack is in progress,

(b) P(t) is the number of packets in transmission within the pre-specified time interval from some time t, and if the ratio of N(t) to P(t) is greater than[[,]] or equal to[[,]] ~~some~~ a second pre-specified threshold k_2, that is, $N(t)/P(t) \geq k_2$, it will be judged that an attack is in progress,

(c) $P(t_1)$ is the number of packets in transmission within the pre-specified time interval from the time t_1, and if the ratio of the coefficient computed in (b) above for the time t

to that computed for the time t1, $\{N(t)/P(t)\} / \{N(t_1)/P(t_1)\}$, is greater than[[,]] or equal to[[,]] ~~some~~ a third pre-specified threshold k_3, that is, $\{N(t)/P(t)\} / \{N(t_1)/P(t_1)\} \geq k_3$, it will be judged that an attack is in progress, and

(d) T(t) is the number of octets or bits in the packets in transmission within the pre-specified time interval from some time t, and if the ratio N(t) to T(t) is greater than[[,]] or equal to[[,]] ~~some~~ a fourth pre-specified threshold k_4, that is, $N(t)/T(t) \geq k_4$, it will be judged that an attack is in progress.

21. (currently amended) The method of claim 20, wherein,

said examining step examines a resultant composite field ~~comprised of~~ comprising arbitrary combinations of two or more of header fields, and

the number of distinct values observed for the resultant composite field is used to compute the coefficient which is compared against the threshold.

22. (currently amended) The method of claim 20, comprising the further steps of:

from an examined packet, inferring that the unauthorized attack is underway when a Time To Live (TTL) value in the pre-specified field of the examined packet is outside a

range of the values seen beforehand for the source address in the header of the examined packet, and

after determining that the source address in the header of the examined packet is legitimate, detecting the unauthorized attack based on whether the ~~Time To Live~~ TTL value is within a pre-specified range of the expected ~~Time To Live~~ TTL value for the source address.

23. (canceled)

24. (currently amended) A method ~~of~~ for detecting a network attack, comprising the step of:

observing values of packet header fields and upon observing that a number of distinct values seen in a combination of two or more header fields exceeds a pre-specified threshold value within a pre-specified time, judging that an unauthorized attack is in progress.

25. (currently amended) The method of claim 24, wherein[[,]] ~~observing~~ a Time To Live (TTL) value in the packet header is observed, and ~~judging~~ the unauthorized attack ~~is~~ in progress is judged upon the observed ~~Time To Live~~ TTL value being outside a range of the values seen beforehand for the source address in the packet header.

26. (canceled)